

## REMARKS/ARGUMENTS

The Applicant acknowledges, with thanks, the office action dated October 31, 2008, and completion of the personal interview of December 16, 2008. The Examiner's observations and suggestions are much appreciated and summarized herein. The Examiner's consideration of Applicant's arguments filed July 17, 2008, is noted with appreciation. Claims 1, 3-9, 11-16, 23, and 25-28 are currently pending.

Claim 9 has been amended to correct a typographical error. No new matter has been added.

Claims 1, 3-9, 11-16, 23, and 25-28 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. It was the Examiner's position that the specification does not disclose receiving an access control list from the associated user and authenticating login data against the access control list. The applicants respectfully traverse. Figure 3 is directed to interaction with the user of the services. Please note block 312 wherein identity information is input of users authorized to access the generated image data. Also, note paragraph 24 which discloses that the authorized person must enter the user identification and password in order to access the image in the secure storage medium and that the authentication and approval of the information is then performed. As such, the specification does disclose these limitations and this rejection should be withdrawn.

Claims 1, 3-9, 11-16, 23, and 25-28 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. It was the Examiner's opinion that the specification does not disclose collaborative access. Claims 1, 9, and 23 have been amended to provide sharing of access. As such, this rejection should be overcome.

Claims 1, 4-8, 9, 12-16, 23, and 25-28 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,254,606 to Hamada (*hereinafter*, "Hamada") in view of U.S. Patent No. 7,225,263 to Clymer et al. (*hereinafter*, "Clymer"). Claims 3, 11, 19, and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Hamada in view of Clymer, and further in view of U.S. Patent Application Publication No. 2003/0071900 to Aoyagi (*hereinafter*, "Aoyagi"). In view of the amendments and arguments set forth below, it is submitted that all pending claims are patentably distinct over the art of record.

The subject application is directed to a system and method for providing selective fee-based sharing of access to data stored on a shared data peripheral device. A storage area is allocated in a secure data storage medium and login data is received corresponding to an identity of an associated user. Formatting data is received from the user corresponding to a format for storage of electronic document data and data received from the associated user is communicated via at least one data input/output device in a data peripheral system into the storage area of secure data storage medium. Charge information is secured from the associated user, which charge information allows for securing of payment for use the data peripheral system and charge verification information is secured corresponding to receive charge information. Operation of the data peripheral system is then enabled in accordance with an output of the verification so as to provide fee-based access of the associated user to the peripheral system. An access control list is received from the user corresponding to an identity of at least one user selected by the associated user as authorized to have future access to the electronic document data stored in the storage area of the secure data storage medium and stored, wherein the access control list, which access control list dictates an identity of users authorized to access the data stored in the storage area of the secure data storage medium. Secure login data is generated for each authorized user associated with the access control list and communicated to each authorized user. Login data is received from the at least one authorized user, authenticated against the access control list, and the electronic document data stored in the storage area of the secure data storage medium is communicated to the at least one authorized user in accordance with an output of the authenticating.

As discussed during the Interview the newly added Clymer patent was cited as teaching a deficiency in Hamada relative to receiving an access control list from an associated user. However, Clymer has a preset access control list that limits accessibility of network devices. The subject application, conversely, teaches a user-specified access control list that sets forth access rights to a particular electronic document.

Amendment has been made to each of independent claims 1, 9 and 23 have been made to clarify that an access list is selected by a user in connection with a particular electronic document. This personal nature of the choice of entries in the access list, as well as the tie of the access list to an electronic document, renders the claims patentably distinct over Hamada and


Clymer, alone or in combination. The deficiencies of Hamada and Clymer are not remedied by the teachings of Aoyagi.

In accordance with the afore-noted amendments and comments, it is submitted that all claims are patentably distinct over the art, and in condition for allowance thereover. An early allowance of all claims is respectfully requested.

If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 66329/00170.

Date: 12/19/08

Respectfully submitted,

  
\_\_\_\_\_  
Susan L. Mizer  
Registration No. 38,245  
TUCKER ELLIS & WEST LLP  
1150 Huntington Bldg.  
925 Euclid Ave.  
Cleveland, Ohio 44115-1414  
**Customer No.: 23380**  
Tel.: (216) 696-3466  
Fax: (216) 592-5009